(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 593 386 A2**

(12) EUROPEAN PATENT APPLICATION

(21) Application number : **93480135.8**

(51) Int. Cl.[5] : **G06F 1/00**

(22) Date of filing : **21.09.93**

(30) Priority : **16.10.92 US 962366**

(43) Date of publication of application :
20.04.94 Bulletin 94/16

(84) Designated Contracting States :
DE FR GB IT

(71) Applicant : **INTERNATIONAL BUSINESS MACHINES CORPORATION**
Old Orchard Road
Armonk, N.Y. 10504 (US)

(72) Inventor : **Fitzpatrick, Greg P.**
101 Civic Center Drive, NY No 422
Rochester, MN 55906 (US)
Inventor : **Haynes, Thomas R.**
806 Forestcrest Court
Euless, TX 76039 (US)
Inventor : **Williams, Marvin L.**
1152 Settlers Way
Lewisville, TX 75067 (US)

(74) Representative : **de Pena, Alain**
Compagnie IBM France Département de Propriété Intellectuelle
F-06610 La Gaude (FR)

(54) Method and apparatus for accessing touch screen desktop objects via fingerprint recognition.

(57) A method of manipulating and obtaining access to graphical desktop objects is disclosed. Touch-sensitive fields are provided on a computer display for user selection. Upon selecting one of the fields with a fingertip, a fingerprint therefrom is analyzed and compared to a list of authorized fingerprints. Once the fingerprint passes inspection, the user is granted access to the underlying program.

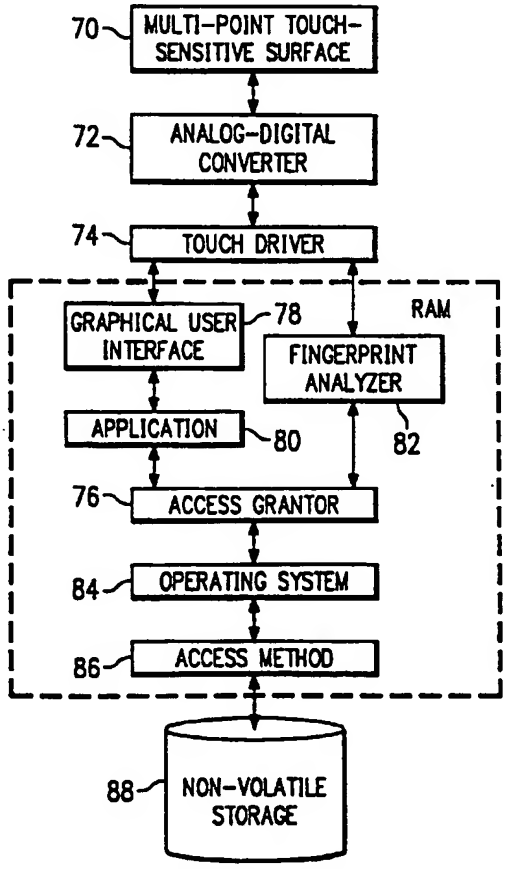


FIG. 4

EP 0 593 386 A2

This invention relates in general to graphical user interfaces, and in particular to the use of fingerprint recognition with touch screens to manipulate graphical desktop objects and to access the underlying data.

Modern computer systems are becoming more user-friendly through the use of graphical user interfaces. Such interfaces provide a more intuitive method for an operator to use the programs thereon. For example, an operator may invoke a program by the selection of a graphical object or icon rather than by typing in a program command. Thus, the operator does not need to remember program commands which are frequently non-intuitive and are generally considered unfriendly.

As computers are more and more widely accepted, more information, including sensitive or classified information, is placed on computers. As is well known, there are many people who pride themselves in the ability to "break" into computer systems to access data. There are many different ways to attempt to prevent unauthorized personnel from obtaining data on a computer. Passwords are commonly used for such a purpose. For example, an operator is required to type in a predetermined code word or sequence of keystrokes before access is granted. If the password is approved, the operator is then allowed to obtain the data and/or run programs as desired. Unfortunately, as noted above, there are many personnel who pride themselves in being able to break code words or passwords and obtain unauthorized entry into computer systems.

In addition to the use of passwords, other entry authorization techniques include the use of identification cards (US Patent No. 4,599,509, July 8, 1986, to Silverman, et al.) and encryption devices (US Patent No. 4,691,355, September 1, 1987, to Wirstrom, et al.).

Whenever a plurality of personnel have access to a single input device, there is a possibility that unauthorized access may be allowed. For example, an operator will typically initialize the terminal at the beginning of the day and sign on with the appropriate password. Thus, access will be granted to any programs to which that operator is allowed by anyone who would use that terminal. If the operator is absent from the terminal, any person authorized or unauthorized would be able to obtain data therefrom. Thus, there is a need for a method and apparatus which will allow a computer system to grant access to individual files/programs on an as-authorized basis only.

Further in the desire to create a more user-friendly system, touch screen technology enables direct object selection by a user's fingers contacting a touch screen surface directly over a graphical object. In addition, there are known devices which can compare a live fingerprint against a referenced print. Thus, while there are fingerprint recognition devices, there is no presently known method and apparatus allowing access to computer systems and individual programs thereon by fingerprint recognition on touch screens.

The present invention provides a method and apparatus for obtaining access to a computer system which eliminates or substantially reduces the problems of the prior art. The present invention allows a computer system, with multiple operators through single input devices, to grant access to individual files/programs on an as-authorized basis only.

In accordance with one aspect of the present invention, a method of obtaining access to a computer system is provided. A recognition device is linked to the system. Access to the system is then based upon an acceptable response provided by a user to the recognition device.

In one embodiment, the recognition device comprises a fingerprint recognition device. By touching a screen directly over a graphical object, a user may be granted access to the program identified thereby only if there is a match with a file of authorized prints. If no match occurs, access to that program is denied. Thus, multiple users of a single terminal can obtain information only from programs to which they are authorized access.

It is a technical advantage of the present invention in that multiple users of a single terminal will be allowed to access only the data they are authorized. It is a further technical advantage of the present invention that access can be granted to multiple levels of information, if authorized, without the need for multiple passwords.

For a more complete understanding of the present invention and the advantages thereof, reference is now made to the Detailed Description taken in conjunction with the attached Drawings, in which:

Figure 1 is a graphical representation of a data processing system in accordance with the present invention;

Figure 2 illustrates a password entry to gain access to a computer system in accordance with the prior art;

Figure 3 illustrates an embodiment of the present invention;

Figure 4 is a diagram illustrating the interrelationship of the various components used in conjunction with the present invention; and

Figure 5 is a flowchart of the present invention.

Referring first to Figure 1, there is depicted a graphical representation of a data processing system 8 which may be utilized to implement the present invention. As may be seen, data processing system 8 may include a plurality of networks, such as Local Area Networks (LAN) 10 and 32, each of which preferably includes a plurality of individual computers 12 and 30, respectively. Of course, those skilled in the art will appreciate that a plurality of Intelligent Work-

stations (IWS) coupled to a host processor may be utilized for each such network. As is common in such data processing systems, each individual computer may be coupled to a storage device 14 and/or a printer/output device 16.

The data processing system 8 may also include multiple mainframe computers, such as mainframe computer 18, which may be preferably coupled to LAN 10 by means of communications link 22. The mainframe computer 18 may also be coupled to a storage device 20 which may serve as remote storage for LAN 10. Similarly, LAN 10 may be coupled via communications link 24 through a subsystem control unit/communications controller 26 and communications link 34 to a gateway server 28. Gateway server 28 is preferably an individual computer or IWS which serves to link LAN 32 to LAN 10.

With respect to LAN 32 and LAN 10, a plurality of documents or resource objects may be stored within storage device 20 and controlled by mainframe computer 18, as resource manager or library service for the resource objects thus stored. Of course, those skilled in the art will appreciate that mainframe computer 18 may be located a great geographic distance from LAN 10 and similarly, LAN 10 may be located a substantial distance from LAN 32. For example, LAN 32 may be located in California while LAN 10 may be located within Texas and mainframe computer 18 may be located in New York.

Referring next to Figure 2, a monitor 40 and keyboard 42 such as found with individual computers 12 and 30 (see Fig. 1) are illustrated. As shown on screen 44 of the monitor 40, a required "Enter Password" as indicated by reference numeral 46 is displayed. In order to gain access to the data accessible through the monitor 40, an operator must type, using keyboard 42, the authorized password in the space provided on the screen 44. As used herein, an "operator" is defined as a person who uses a computer program installed on a computer system. The term "user" may be used interchangeably herein to mean the same as an "operator". Once the proper password is typed, entered and accepted, the operator typically has access to any information available thereby. Thus, if the operator leaves the monitor 40 unattended without appropriately securing same, an unauthorized person may obtain access to data therethrough.

Referring to Figure 3, a monitor 50 and keyboard 52 such as are used with the individual computers 12 and 30 (see Fig. 1) are illustrated. In contrast with the prior art, the present invention does not provide access to all data available through the monitor 50 just by entering a single (or even multiple levels) of code words. Once the computer system to which the monitor 50 and 52 has been activated, touch screen fields (which may include text or graphics) are presented to the operator. For example, a touch screen field 54 is provided for access to confidential files, a touch screen field 56 is provided for access to secret files and a touch screen field 58 is provided for access to unclassified files. In addition, touch screen fields 60, 62, 64, 66 and 68 may be provided for access to programs/data A, B, C, D and E, respectively. In order to gain access to any of the data or programs indicated by one of the touch screen fields 54, 56, 58, 60, 62, 64, 66 or 68 an operator must place their fingertip thereon. At that point, a fingerprint recognition device interconnected to the monitor 50 will check for authorized access. If the operator is authorized access to that data/program, the data/program will be presented to the operator. Any single operator may be authorized access to one or more of the programs/files presented on the monitor 50. Similarly, all operators in a department/group may access data/programs through the monitor 50 only if they are authorized for the specific information they are attempting to gain access to. By using the present invention, the unattended monitor 50 has a reduced likelihood of being used to compromise data by personnel not authorized access thereto. Also, use of a time delay may keep unattended access to a specific program (already opened) to a minimum.

Referring to Figure 4, a graphical illustration of the interrelationship of components necessary to utilize the present invention is illustrated. A multi-point, touch-sensitive surface 70 which detects contact at given points is provided with the monitor 50 (see Fig. 3). An analog-digital converter 72 to pass data about contacts is positioned between the touch-sensitive surface 70 and a touch driver 74. From the touch driver 74, a dual path is taken to an access grantor 76. In a first path, a graphical user interface 78 indicates which icon has been selected. Information about the selected icon is then passed to an application 80 for processing. In a second path, the touch driver 74 communicates with a fingerprint analyzer 82. A fingerprint image is communicated to the analyzer 82 in a form appropriate to distinguish a unique fingerprint, as is known in the art. Once an operator touches a field or an icon, a fingerprint template is compared to an associated "per-icon" access table found in the access grantor 76. Upon the templates meeting a specified confidence level, manipulation access is granted through an operating system 84 and access method 86. The appropriate program/data is then obtained from nonvolatile storage 88 which allows the operator to proceed.

Referring to Figure 5, a flowchart illustrating the present invention is provided. The present invention starts at 100 and waits for user interaction at block 102. At decision block 104 it is determined whether or not an "End Program" is detected. If the response to decision block 104 is yes, the present invention ends at 106. If the response to decision block 104 is no, the operating system is queried for selected object identification at block 108.

At decision block 110 it is then determined whether or not the object ID requires fingerprint authentication or not. If the response to decision block 110 is no, the program associated with the selected object is invoked at block 112 which is an unlimited capability followed by a return to block 102 to wait for user interaction. If the response to decision block 110 is yes, an image is obtained from the touch driver at block 114.

At decision block 116 it is determined whether or not the image meets the recognition threshold. If the response to decision block 116 is no, an error message is returned to the user at block 118 followed by a return to block 102. If the response to decision block 116 is yes, it is determined at decision block 120 whether or not an image match is found within the access table domain. If the response to decision block 120 is no, an error message is returned to the user at block 118 followed by a return to block 102. If the response to decision block 120 is yes, it is determined at decision block 122 whether or not the access table contains a recognized user and selected object match. If the response to decision block 122 is no, an error message is returned to the user at block 118 followed by return to block 102. If the response to decision block 122 is yes, it is determined at decision block 124 whether or not the access table contains application usage restrictions for this user. If response to decision block 124 is yes, programs associated with the selected object (a limited capability) are invoked at block 126 followed by a return to block 102. If the response to decision block 124 is no, the program associated with the selected object is invoked at decision block 112 followed by a return to block 102.

As a result of the present invention, security of a terminal and the programs accessed thereby is greatly enhanced. To access data available through the terminal, a user must be authorized access and must in fact be the authorized user as evidenced by a fingerprint. Once a terminal is initiated, a user may leave the terminal unattended with reduced fear of unauthorized access to sensitive information. Even if the user leaves the terminal with a sensitive program running thereon, an unauthorized user would be unable to access other data. By including a timer, unattended access by unauthorized personnel will be cut even further.

Claims

1. A method of obtaining access to a computer system, comprising the steps of:
   linking a recognition device to the system; and
   allowing access to the system based upon an acceptable response provided by a user to said recognition device.

2. The method of Claim 1, wherein said step of linking comprises:
   installing a fingerprint recognition device.

3. The method of Claim 1, further comprising the step of:
   locking the system after a predetermined amount of time has lapsed without any user interaction.

4. A method of manipulating data availability on a computer system, comprising the steps of:
   selecting a touch screen field displayed on the system with a user's fingertip;
   comparing a fingerprint from said fingertip with an access table containing representations of fingerprints authorized access to said field; and
   granting access if said fingerprint matches one of said fingerprints authorized access.

5. The method of Claim 4, wherein said step of selecting a field comprises:
   selecting a graphical object.

6. The method of Claim 4, wherein said step of selecting a field comprises:
   selecting a textual field.

7. A device for granting access to a computer system, comprising:
   means for linking a recognition device to the system; and
   means for allowing access to the system based upon an acceptable response provided by a user to said recognition device.

8. The device of Claim 7, wherein said means for linking comprises:
   a fingerprint recognition device;
   an analog-digital converter; and
   a touch driver.

9. The device of Claim 7, wherein said means for allowing access comprises:
   means for indicating a selected data field; and
   means for comparing a user response to an acceptable response for said data field.

10. The device of Claim 9, wherein said means for indicating a selected data field comprises:
    a graphical user interface; and
    an application.

11. The device of Claim 10, wherein said means for comparing comprises:
    a fingerprint analyzer; and
    an access grantor.

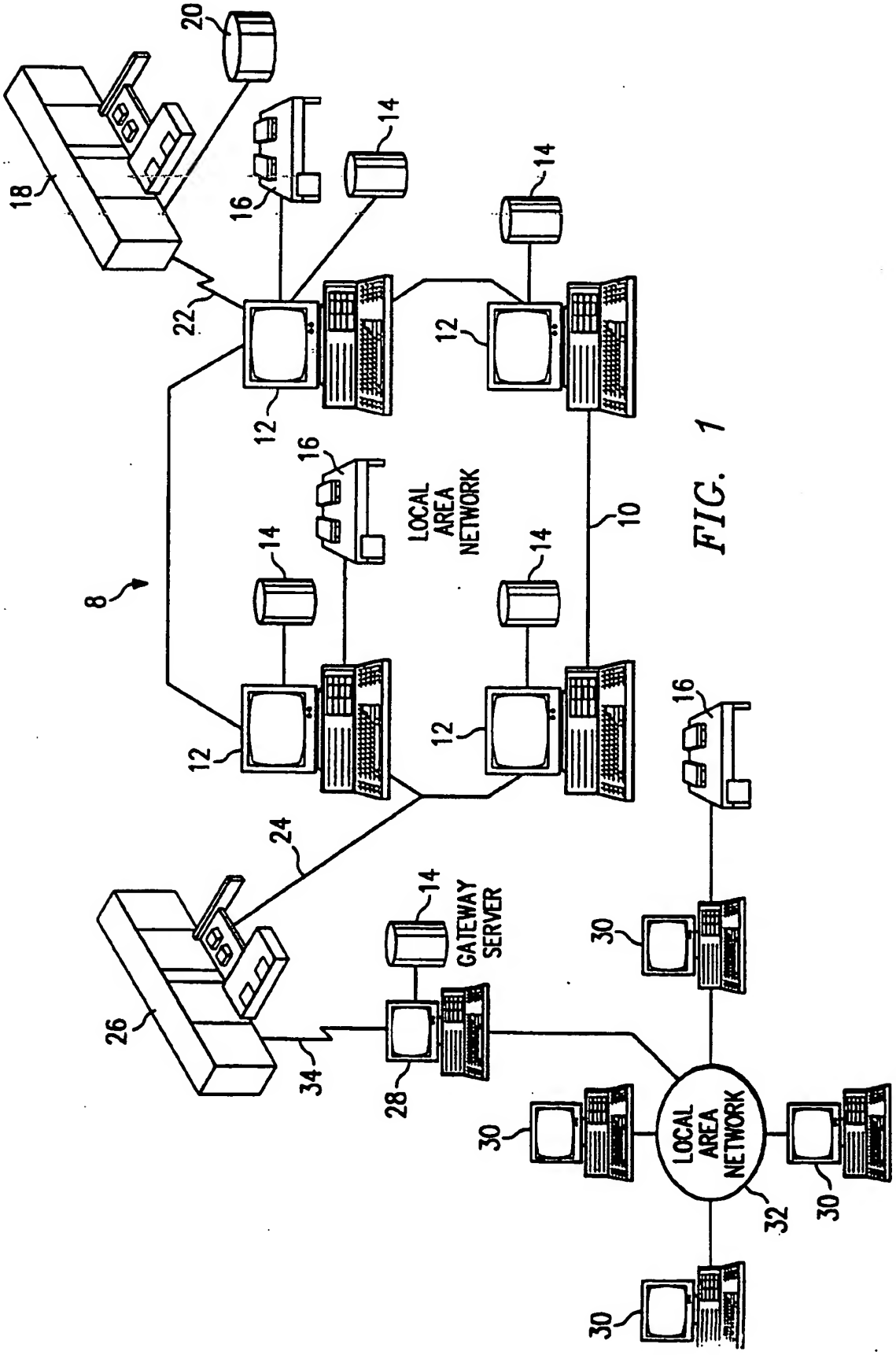

20
18
16
14
22
12
14
12
16
LOCAL AREA NETWORK
8
14
14
10
12
12
16
24
14
GATEWAY SERVER
26
30
34
28
30
LOCAL AREA NETWORK
32
30
30

FIG. 1

FIG. 2
(PRIOR ART)

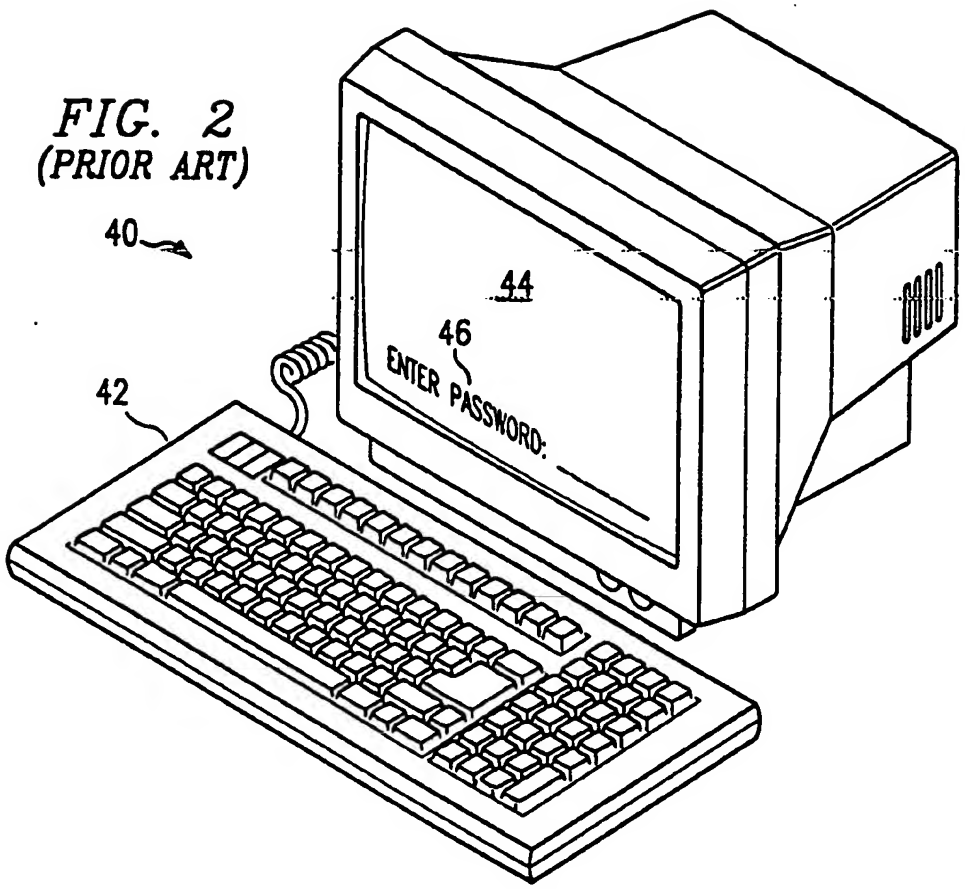
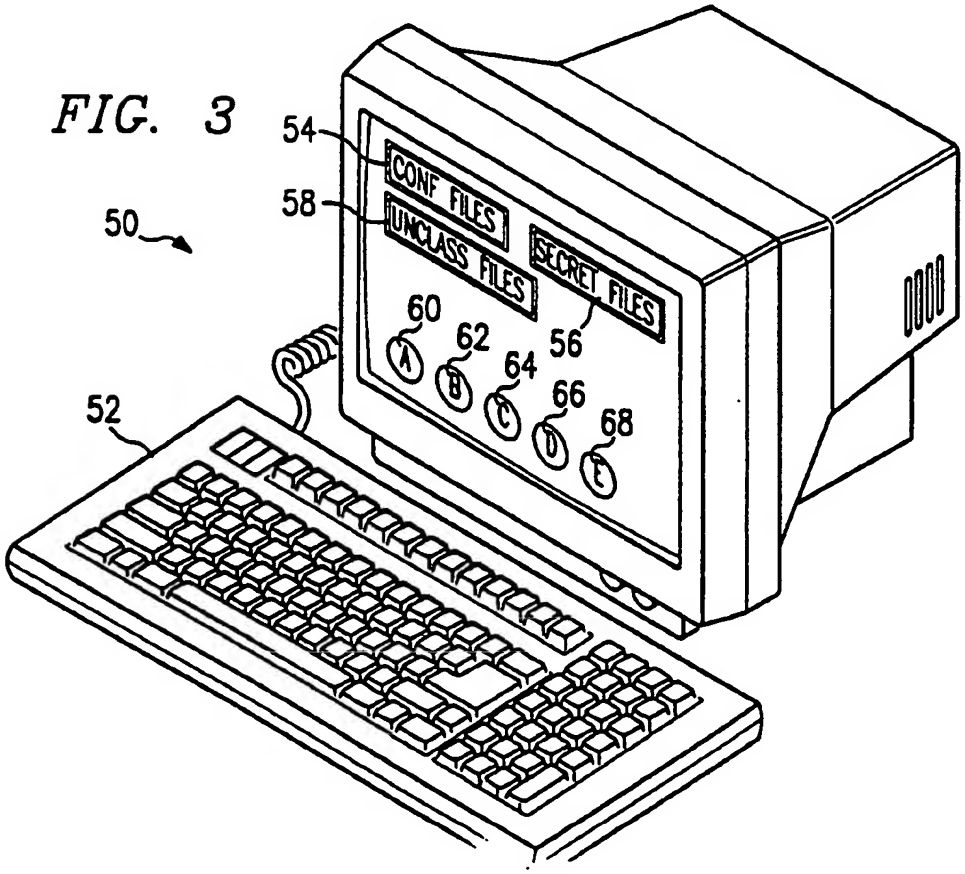


FIG. 3



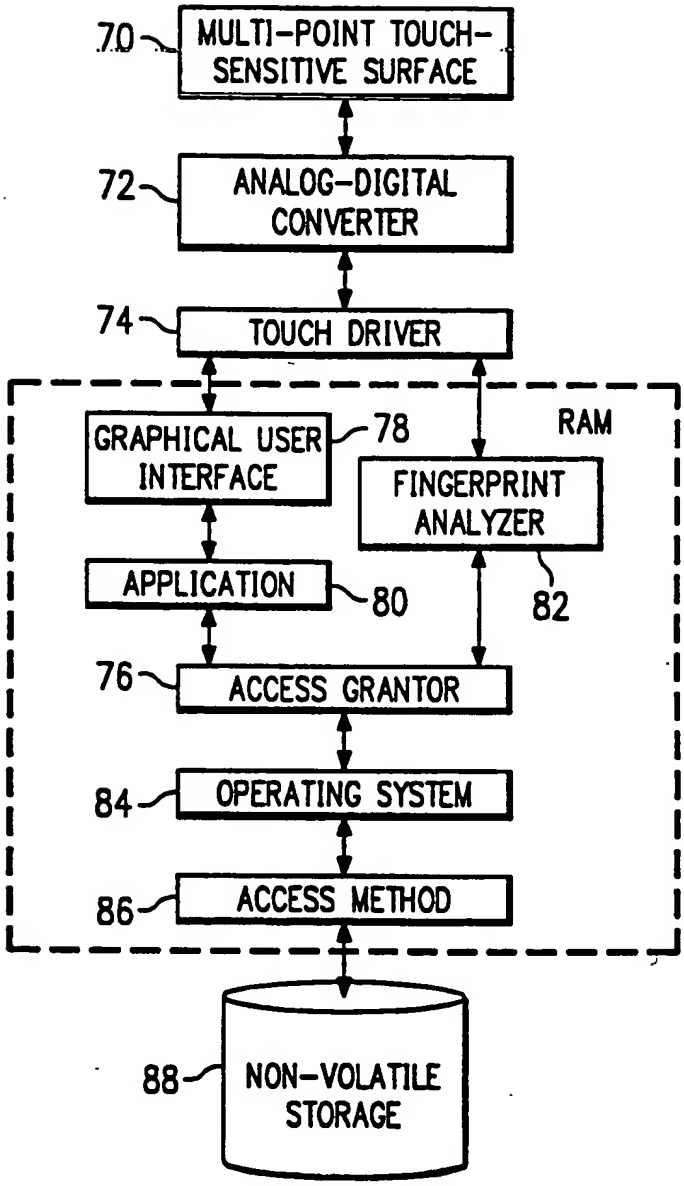

70
MULTI-POINT TOUCH-SENSITIVE SURFACE
72
ANALOG-DIGITAL CONVERTER
74
TOUCH DRIVER
GRAPHICAL USER INTERFACE
78
RAM
FINGERPRINT ANALYZER
APPLICATION
80
82
76
ACCESS GRANTOR
84
OPERATING SYSTEM
86
ACCESS METHOD
88
NON-VOLATILE STORAGE

FIG. 4

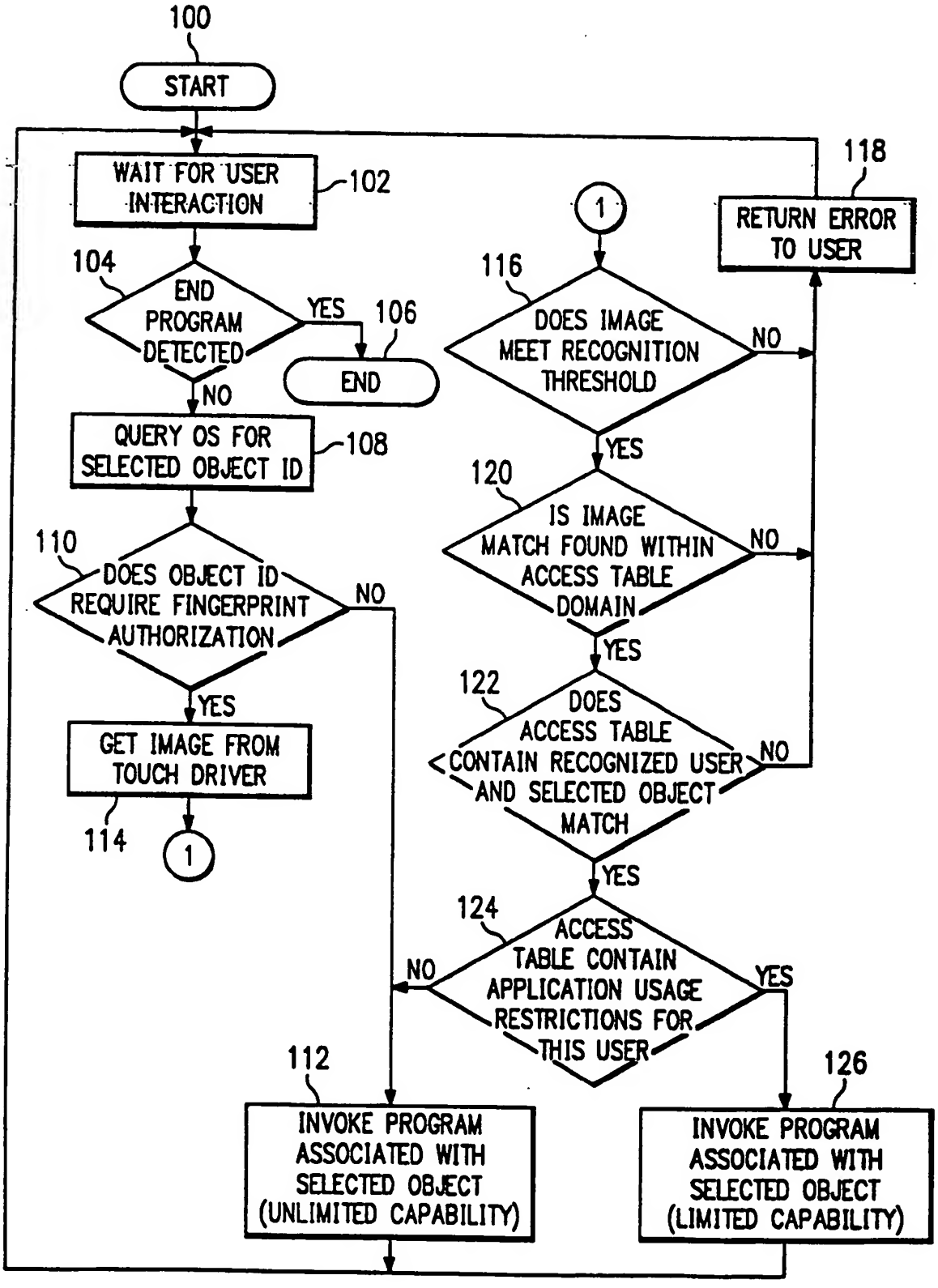

100
START
WAIT FOR USER INTERACTION
102
104
END PROGRAM DETECTED
YES
106
END
NO
QUERY OS FOR SELECTED OBJECT ID
108
110
DOES OBJECT ID REQUIRE FINGERPRINT AUTHORIZATION
NO
YES
GET IMAGE FROM TOUCH DRIVER
114
1
1
116
DOES IMAGE MEET RECOGNITION THRESHOLD
NO
YES
118
RETURN ERROR TO USER
120
IS IMAGE MATCH FOUND WITHIN ACCESS TABLE DOMAIN
NO
YES
122
DOES ACCESS TABLE CONTAIN RECOGNIZED USER AND SELECTED OBJECT MATCH
NO
YES
124
ACCESS TABLE CONTAIN APPLICATION USAGE RESTRICTIONS FOR THIS USER
NO
YES
112
INVOKE PROGRAM ASSOCIATED WITH SELECTED OBJECT (UNLIMITED CAPABILITY)
126
INVOKE PROGRAM ASSOCIATED WITH SELECTED OBJECT (LIMITED CAPABILITY)

FIG. 5